

Examining the Role of Critical Infrastructure/Cybersecurity

Chairman's Presentation March 3, 2021



Gladys Brown Dutrieuille, Chairman
Pennsylvania Public Utility Commission



**Gladys Brown
Dutreuille**
Chairman



David Alexander
Legal Counsel
to the Chairman



Damon P. Anderson
Chief Information Officer



Mike Holko
Director of the Office of
Cybersecurity, Compliance
and Oversight



June Perry
Director of Legislative
Affairs



Tom Beene
Deputy Director
of Legislative Affairs

Cybersecurity Overview

Recent Cyber Events:

- **Feb. 5, 2021** - A water treatment plant in Oldsmar, Florida, experienced a cyberattack which was intended to gain control over the Supervisory Control and Data Acquisition (SCADA) systems used to monitor and regulate the amount of sodium hydroxide within the water supply. Sodium hydroxide is used for pH adjustment and can be harmful at high concentrations.
- **December 13, 2020** - A SolarWinds product, Orion, used by about 33,000 public and private sector customers. The attack persisted undetected for months in 2020, and additional details about the breadth and depth of compromised systems continued to surface after the initial disclosure.
- **March 6, 2020** - Ryuk ransomware infected Durham NC city and county networks after employees clicked on phishing emails. Around 100 servers from the county's data center will have to be rebuilt and 1,000 computers will have to be re-imaged.
- **March 1, 2020** - Cyberattack impacted email accounts and server function for the City of Torrance. The attack rendered the city unable to update the website or process credit card payments.

Cybersecurity Overview

Utility Threat Landscape/Environment

- Physical infrastructure is a growing target
 - Utility and power companies' industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems under increasing attack
- An ICS or SCADA attack could lead to extended and large-scale service outages
- A cyber-attack could cripple a utility and have a dangerous domino effect for consumers
 - Fortunately, in the utility industry, these breaches have not resulted in any significant repercussions in the U.S. – yet

PUC Cybersecurity Regulations

- **Confidential Security Information Disclosure Protection Act (CSI Act) (35 P.S. § 2141)** – The CSI Act specifically defines Confidential Security Information (CSI) to include, among other things, vulnerability assessments, emergency response plans, and security plans. The CSI Act directs the Pennsylvania Public Utility Commission (PA PUC) to develop filing protocols and procedures for public utilities to follow when filing CSI with the Commission, and to address challenges to the designations or requests to examine records containing CSI.
- **Cybersecurity Plans and Self-Certification Regulations (52 Pa. Code § 101.1 - 7)** – These regulations require jurisdictional utilities to develop and maintain written physical, cybersecurity, emergency response, and business continuity plans. They also require utilities to submit a Public Utility Security Planning and Readiness Self-Certification Form on an annual basis.

PUC Cybersecurity Regulations (continued)

- **Cybersecurity Incident Reporting (52 Pa. Code § 57.11(b)(4), 59.11(b)(5) and 65.2(b)(4))** – These regulations require jurisdictional electric, natural gas, water and wastewater utilities to report an occurrence of an unusual nature that is a physical or cyber attack, including attempts against cybersecurity measures as defined in Chapter 101, which causes an interruption of service or more than \$50,000 in damages.
- **Management Audits (66 Pa. Code § 516)** – The PA PUC's Bureau of Audits conducts Management Audits on the utilities' cybersecurity, emergency preparedness, physical security, and business continuity plans. Any deficiencies identified during the audit are reviewed during a post audit review with the utility, and the PA PUC follows-up with the utility to ensure that corrective action is taken to address the deficiencies.

PUC Cybersecurity History 2003 - Present

- 2003 – Final Order issued on Physical and Cyber Security Program Self Certification Requirements for Public Utilities at Docket No. M-00031717.
- 2004 – Final Rulemaking Order issued on Public Utility Security Planning and Readiness (including cybersecurity readiness) at Docket No. L-00040166. The rulemaking includes a requirement that jurisdictional utilities submit self-certification forms to the Commission.
- 2005 – Commission regulations enacted and found at 52 Pa. Code § 101 – Public Utility Preparedness Through Self Certification, which requires jurisdictional utilities to develop and maintain appropriate written physical security, cybersecurity, emergency response and business-continuity plans to protect the Commonwealth's infrastructure and the provision of safe, continuous and reliable utility service.
- 2006 – Implementation of the Public Utility Confidential Security Information Disclosure Protection Act to protect utility security information deemed confidential. Confidential security information is not subject to Pennsylvania's Right to Know Law.

PUC Cybersecurity History 2003 – Present (continued)

- 2009 – The Commission clarified jurisdictional utilities’ responsibilities under 52 Pa. Code § 101. The Order clarifies that all utility distribution infrastructure assets must be included in a utility’s cybersecurity plan.
- 2013 – The Commission:
 - Held a collaborative meeting with state and federal agencies (including the Federal Energy Regulatory Commission (FERC), the Federal Communications Commission (FCC), the Pennsylvania State Police (PSP), the PA Governor’s Office of Homeland Security (GOHS), Pennsylvania Office of Administration, etc.) to start a dialogue between the levels of government about roles and support.
 - Established a Middle Atlantic Cybersecurity Collaborative among five states including Delaware, Maryland, Ohio, Pennsylvania and New Jersey, as well as Washington, D.C., to provide opportunities for education and information sharing of cyber incidents affecting the region.
 - Hosted a Cyber Resilience Workshop with cybersecurity experts and jurisdictional water/wastewater, gas, electric and telephone breaches/issues.

PUC Cybersecurity History 2003-Present (continued)

- 2014 – The Commission:
 - Established a Critical Infrastructure Interdependency Working Group (CIIWG). Part of the group's mission is for utilities and other affected parties to report and coordinate necessary actions in response to cyber incidents.
 - Released Cybersecurity Best Practices for Small and Medium Pennsylvania Utilities – a document tailored toward providing cybersecurity advice, as well as information on resources for small- to medium-sized utilities (Updated in 2015 and 2020).
- 2015 – The Commission:
 - Signed a Memorandum of Understanding with PSP to become an active participant in PSP's Fusion Center in order to enhance the information-sharing process between the two agencies regarding both physical and cybersecurity concerns.
 - Organized and hosted a cyber-awareness event that involved several state and federal government agencies, utility companies and law enforcement.

PUC Cybersecurity History 2003-Present (continued)

- 2016 – The Commission conducted a cross sector Black Sky Training Exercise for regulated utilities in conjunction with the Office of the Governor.
- 2018 – The Commission:
 - Hired a Director for the Office of Cybersecurity Compliance and Oversight.
 - Established the Cybersecurity Outreach program to help small and medium utilities with their cybersecurity preparedness.
- 2019 – The Commission hosted its first cybersecurity conference.
- 2020 – Updated the Bureau of Audits cybersecurity workplan, aligning the Bureau's efforts with the NIST Cybersecurity Framework.
- 2020 – Updated the Commission's internal protocols for utility reports on cybersecurity breaches/issues.

PUC Cybersecurity Initiatives – Internally Facing

A NIST 800-53 Based Security Program

Defends the PUC’s Data, Systems and People

Management	Operational	Technical
Data Classification	Security Awareness and Training	Identity Management and Access Control
Planning and Program Management	Vulnerability and Threat Management	Identification and Authentication
System and Services Acquisition	Incident Response	Audit and Accountability
Risk Management	Business Continuity Planning / COOP	Change and Configuration Management
Security Assessment and Authorization	Personnel Security	System Security Maintenance
	Media Protection	System and Information Integrity
	Secure Software Development Lifecycle	System and Communications Protection
	Physical and Environmental Security	

PUC Cybersecurity Initiatives – Internally Facing

Yesterday's Accomplishments will not Protect Us Tomorrow

Past

- ✓ Established Internal Security Team
- ✓ Launched Vulnerability and Threat Management Program
- ✓ Conducted NIST 800-53 Assessment – 800 controls/18 Domains
- ✓ Conducted Penetration Testing with PaNG
- ✓ Identified Areas to Strengthen Security Architecture
- ✓ Deliver Cyber Awareness, Training and Education Program

Present

- Developing 3 Year Security Plan to Address Identified gaps
- Developing Information Security Policy Set
- Applying NARUC Cyber Strategy Development Guidance to Internal Program with Carnegie Mellon Student Team
- Strengthening Cybersecurity Architecture
- Conduct Penetration Testing with PaNG – Series 3

Future

- Execute 3 Year Security Plan
- Implement NARUC Risk Management Best Practices
- Evolve Incident Response to Constantly Advancing Threat Landscape
- Invest in Breadth and Depth of Internal Security Team
- Continue Strengthening Cybersecurity Architecture

PUC Cybersecurity Initiatives – Internally Facing

Showcase: Cyber Security Awareness and Training Program

Goal: Prepare Commission Staff to be the First Line of Defense and Build a Security Culture

Learning Objectives	Components	Tools/Resources	Metrics
<ul style="list-style-type: none"> Common Attack Vectors Human Factors & Insider Threats Operational & Technical Risks Scams & Phishing 	<ul style="list-style-type: none"> On-going Phishing Exercises Monthly Cyber Threat Tuesday Briefings All User Cyber Messages Bi-weekly Cyber Security Work Group Role Based Custom Programming – Audits / Law Scenarios 	<ul style="list-style-type: none"> Cybrary - Education Programs FedVTE – Free for Government Employees KnowBe4 PhishMe NARUC Cybersecurity Training Programs 	<ul style="list-style-type: none"> Phishing Click Rates % Commission Staff Attending Awareness Activities % Commission Staff Trained

PUC Cybersecurity Initiatives - Externally Facing

- **PUC Cybersecurity Outreach Program** – The Commission’s Cybersecurity Outreach Program provides the regulated utilities with information about the latest cybersecurity threats, industry best practices, cyber resiliency, etc.
- **Annual PUC Cybersecurity Conference** – The Commission created an annual Cybersecurity Conference to help ensure that the Commonwealth’s regulated utilities are protected from cyber-attacks.
- **Cybersecurity Regulated Utility Threat Briefing** – The Commission is working with the Department of Homeland Security, Critical Infrastructure Security Agency (DHS-CISA), Electric Information Sharing and Analysis Center (E-ISAC), Multi State ISAC, and the Pennsylvania Criminal Intelligence Center to provide the regulated utilities and PUC staff with quarterly cybersecurity threat briefings.
- **Externally Facing Utility Cybersecurity Incident Response Plan** – The Commission created an internal cybersecurity plan that ensures the PUC has coordinated communications with internal and external stakeholders. The plan also ensures that the internal response aligns with our responsibilities in the Commonwealth Emergency Operations Plan and the Pennsylvania Cyber Incident Annex.
- **Bureau of Audits Cybersecurity Management Audit** – The Commission updated the Bureau of Audits cybersecurity assessment was updated to incorporate questions from the National Institute of Standards and Technology (NIST), Cybersecurity Framework. This enabled the Bureau of Audits to standardize their assessment process

PUC Cybersecurity Initiatives - Externally Facing

- **Title 52 – Cybersecurity Incident Reporting Regulations** – The Commission's regulations require jurisdictional electric; natural gas; and water and wastewater utilities (52 Pa. Code §§ 57.11 (b)(4), 59.11(b)(5) and 65.2(b)(4) to report an occurrence of an unusual nature that is a physical or cyber-attack, including attempts against cybersecurity measures as defined in Chapter 101, which causes an interruption of service or over \$50,000 in damages, or both.
- **Utility Cost-Recovery Analysis / Process** – As cybersecurity evolves and additional expensive technology is deployed, it is anticipated that utilities may specifically identify these initiatives or costs within a rate case. In addition, data breaches or other cyber-attacks often result in considerable costs to correct the breach. The Commission looking into a standardized process to make sure cybersecurity costs are prudent.
- **Pennsylvania Information Security Analysis Center (PA-ISAC)** –The Commission is working with the Office of Administration, Office for Information Technology (OA/OIT) to help create a cybersecurity information sharing analysis center that will help coordinate and communicate cybersecurity information threat information to the state agencies and critical infrastructure entities such as the utilities the Commission regulates.

PUC Cybersecurity Training & Tabletop Exercises

- **U.S. Department of Homeland Security** – Cybersecurity and Infrastructure Security Agency (DHS-CISA) Training – DHS-CISA provides utilities and state regulators with cybersecurity training and tabletop exercises. The training and exercises can be in person and online. <https://www.cisa.gov/cybersecurity-training-exercises>
- **North American Electric Reliability Corporation (NERC) Grid Security Exercise (GridEx)** – GridEx provides NERC and state regulators with an opportunity to observe how utilities would respond to and recover from simulated cybersecurity and physical security threats to their critical infrastructure. <https://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx>
- **Electric Infrastructure Security (EIS) Black Sky Training** –EIS leverages video material simulating news and emergency response operations, with interactive moderation based on evolving resilience and response recommendations from the Electric Infrastructure Protection (EPRO) Handbook Series. <https://www.eiscouncil.org/>

PUC Stakeholders

- **Commonwealth Agencies**

- Governor's Office of Homeland Security (GOHS)
- Pennsylvania Emergency Management Agency (PEMA)
- Pennsylvania State Police (PSP)
- PSP - Pennsylvania Criminal Intelligence Center (PaCIC)
- Pennsylvania National Guard (PNG)
- Office of Administration, Office for Information Technology (OA/OIT)
- Pennsylvania Department of Environmental Protection (PA DEP)
- Pennsylvania Department of Labor & Industry (L&I)
- Pennsylvania Department of Transportation (PennDOT)

- **Federal Agencies**

- Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (DHS-CISA)
- Federal Energy Regulatory Commission (FERC)
- Federal Bureau of Investigation (DOJ-FBI)

- **Stakeholders**

- National Association of Regulatory Utility Commissioners (NARUC)
- PJM Interconnection
- Information Sharing and Analysis Centers (ISACs)
 - Multi-State ISAC (MS-ISAC)
 - Electricity (E-ISAC)
 - Oil and Gas (ONG-ISAC)
 - Water ISAC (W-ISAC)